

# Simplified quantum bit commitment using single photon nonlocality

Guang Ping He\*

*School of Physics and Engineering, Sun Yat-sen University, Guangzhou 510275, China*

We simplified our previously proposed quantum bit commitment (QBC) protocol based on the Mach-Zehnder interferometer, by replacing symmetric beam splitters with asymmetric ones. The protocol is immune to the cheating strategy in the Mayers-Lo-Chau no-go theorem of unconditionally secure QBC, because the density matrices of the committed states do not satisfy a crucial condition on which the no-go theorem holds.

PACS numbers: 03.67.Dd, 03.67.Hk, 42.50.Ex, 03.65.Ta, 03.67.Ac, 03.65.Ud, 42.50.St

## I. INTRODUCTION

Quantum bit commitment (QBC) is a two-party cryptography including two phases. In the commit phase, Alice (the sender of the commitment) decides the value of the bit  $b$  ( $b = 0$  or  $1$ ) which she wants to commit, and sends Bob (the receiver of the commitment) a piece of evidence, e.g., some quantum states. Later, in the unveil phase, Alice announces the value of  $b$ , and Bob checks it with the evidence. An unconditionally secure QBC protocol needs to be both binding (i.e., Alice cannot change the value of  $b$  after the commit phase) and concealing (Bob cannot know  $b$  before the unveil phase) without relying on any computational assumption.

QBC is recognized as an essential primitive for quantum cryptography, as it is the building block for quantum multi-party secure computations and more complicated “post-cold-war era” multi-party cryptographic protocols [1, 2]. Unfortunately, it is widely accepted that unconditionally secure QBC is impossible [3]-[26], despite of some attempts towards secure ones (a detailed list can be found in the introduction of [27]). This result, known as the Mayers-Lo-Chau (MLC) no-go theorem, was considered as putting a serious drawback on quantum cryptography.

Very recently, we proposed a QBC protocol using orthogonal states [27, 28], where the density matrices do not satisfy a crucial condition on which the MLC no-go theorem holds. Thus unconditional security becomes achievable. This QBC protocol is based on a quantum key distribution (QKD) scheme proposed by Goldenberg and Vaidman [29], which makes use of the Mach-Zehnder interferometer involving symmetric beam splitters. Koashi and Imoto pointed out [30] that the Goldenberg-Vaidman (GV) scheme can be simplified by replacing the symmetric beam splitters with asymmetric ones. Here we will apply the same idea to simplified our QBC protocol.

## II. NOTATIONS AND SETTINGS

Generally, in both QKD and QBC the two participants are called Alice and Bob. But similar to [27], in our current QBC protocol, the behaviour of Bob is more like that of the eavesdropper rather than the Bob in QKD. To avoid confusion, here we use the names in the following way. In QKD, the sender of the secret information is called Alice, the receiver is renamed as Charlie instead of Bob, and the external eavesdropper is called Eve. In QBC, the sender of the commitment is Alice, the receiver is Bob, and there is no Eve since QBC merely deals with the cheating from internal dishonest participants, instead of external eavesdropping.

As our main interest is focused on the theoretical possibility of unconditionally secure QBC, we will only consider the ideal case where no transmission error occurs in the communication channels, nor there are detection loss or dark counts, etc.

## III. THE KOASHI-IMOTO QKD SCHEME

Our QBC proposal is inspired by the Koashi-Imoto (KI) QKD scheme [30], which makes use of the Mach-Zehnder interferometer illustrated in FIG. 1. Let  $R$  and  $T$  denote the reflectivity and transmissivity of the asymmetric beam splitters  $BS_1$  and  $BS_2$ , with  $R + T = 1$  and  $R \neq T$ . Alice encodes the bit values 0 and 1 she wants to transmit to Charlie, respectively, using two orthogonal states

$$\begin{aligned} 0 &\rightarrow |\Psi_0\rangle \equiv \sqrt{T}|0\rangle_X|1\rangle_Y - i\sqrt{R}|1\rangle_X|0\rangle_Y, \\ 1 &\rightarrow |\Psi_1\rangle \equiv \sqrt{T}|1\rangle_X|0\rangle_Y - i\sqrt{R}|0\rangle_X|1\rangle_Y. \end{aligned} \quad (1)$$

Here  $|n\rangle_j$  is the  $n$  photon Fock state for the arm  $j = X, Y$ . That is, each  $|\Psi_0\rangle$  or  $|\Psi_1\rangle$  is split into two localized wave packets, and sent to Charlie separately in quantum channels  $X$  and  $Y$  respectively, thus single photon nonlocality is presented. This is done by sending a single photon either from the source  $S_0$  (sending  $|\Psi_0\rangle$ ) or  $S_1$  (sending  $|\Psi_1\rangle$ ), then splitting it with the beam splitter  $BS_1$  made of a half-silvered mirror (note that polarizing beam splitters are not recommended due to the security problem addressed at the end of Sec. 6 of [27]).

---

\*Electronic address: hegp@mail.sysu.edu.cn

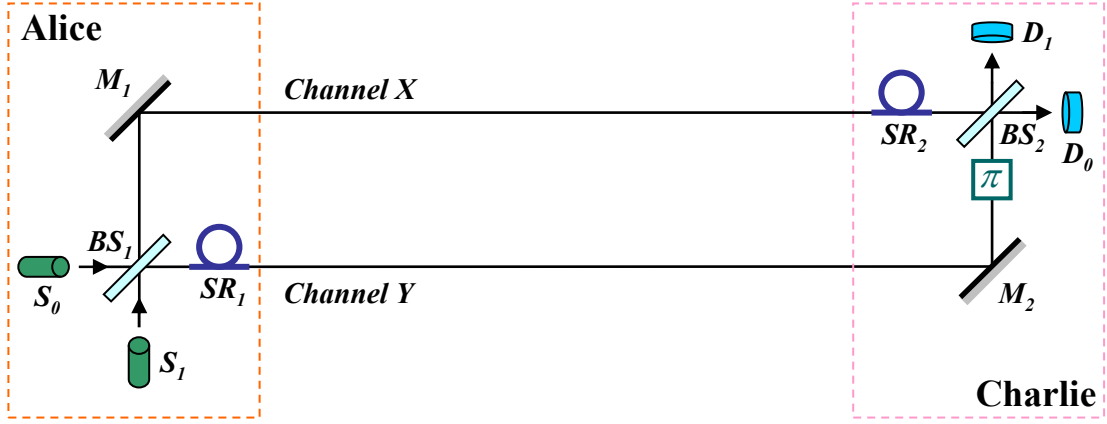


FIG. 1: Diagram of the experimental implementation of the Koashi-Imoto QKD scheme [30]. The state of a photon produced by the source  $S_0$  ( $S_1$ ) will become  $|\Psi_0\rangle = \sqrt{T}|0\rangle_X|1\rangle_Y - i\sqrt{R}|1\rangle_X|0\rangle_Y$  ( $|\Psi_1\rangle = \sqrt{T}|1\rangle_X|0\rangle_Y - i\sqrt{R}|0\rangle_X|1\rangle_Y$ ) after passing the asymmetric beam splitter  $BS_1$ . The two wave packets of the same photon are sent through channels  $X$  and  $Y$  respectively. When no eavesdropper is present, the storage rings  $SR_1$ ,  $SR_2$ , the mirrors  $M_1$ ,  $M_2$  and the phase shifter  $\pi$  will ensure the complete apparatus work as a Mach-Zehnder interferometer, so that  $|\Psi_0\rangle$  ( $|\Psi_1\rangle$ ) will be detected by the detector  $D_0$  ( $D_1$ ) with certainty.

To ensure the security of the transmission, the wave packet in channel  $Y$  is delayed by the storage ring  $SR_1$ , which introduces a sufficiently long delay time  $\tau$  so that this wave packet will not leave Alice's site until the other wave packet in channel  $X$  already entered Charlie's site. Thus the two wave packets of the same photon are never present together in the transmission channels. This makes it impossible for Eve to prepare and send Charlie a perfect clone *on time* if she waits to intercept and measure both wave packets, even though  $|\Psi_0\rangle$  and  $|\Psi_1\rangle$  are orthogonal. On the other hand, when no eavesdropping occurs, Charlie can distinguish  $|\Psi_0\rangle$  and  $|\Psi_1\rangle$  unambiguously by adding a storage ring  $SR_2$  to channel  $X$  whose delay time is also  $\tau$ , while introducing a phase shift  $\pi$  to channel  $Y$ . The two wave packets of the same photon will then recombine and interfere on the beam splitter  $BS_2$ , which is identical to  $BS_1$ . Thus the complete apparatus of Alice and Charlie forms a Mach-Zehnder interferometer, so that  $|\Psi_0\rangle$  ( $|\Psi_1\rangle$ ) will always make the detector  $D_0$  ( $D_1$ ) click with certainty, allowing Charlie to decode the transmitted bit correctly. Any mismatch result between Alice's transmitted state and Charlie's measurement will immediately reveals the presence of Eve [30].

Comparing with the GV QKD protocol [29], the key difference is that  $BS_1$  and  $BS_2$  in the KI scheme are asymmetric beam splitters, while the GV scheme uses symmetric ones. The advantage of this modification is that the sending time of each photon can be fixed and publicly known beforehand, while in the GV scheme it has to be random and kept secret from Eve until the security check.

#### IV. OUR QBC PROTOCOL

As illustrated in FIG. 2, to build a QBC protocol upon the above KI QKD scheme, we treat Charlie's site as a part of Alice's, so that the two parties merge into one. That is, Alice sends out a bit-string encoded with the above orthogonal states, whose value is related with the bit she wants to commit. Then she receives the states herself. Meanwhile, let Bob take the role of Eve. His action shifts between two modes. In the *bypass* mode, he simply does nothing so that the corresponding parts of the states return to Alice intact. In the *intercept* mode, he applies the intercept-resend attack. That is, he intercepts the state and decode the corresponding bit (which can be done by using the same device as that of Charlie's), while prepares a fake state and resends it to Alice on time. Let  $\varepsilon$  denote the lower bound of the average probability for his resend state to be caught in Alice's check. Since the KI QKD scheme was shown to be unconditionally secure [30], it is clear that  $\varepsilon$  cannot always equal exactly to zero for both  $|\Psi_0\rangle$  and  $|\Psi_1\rangle$ , regardless the strategy according to which Bob prepares the resend state. Therefore, Alice can estimate the frequency of the presence of the intercept mode, to limit Bob from intercepting the whole string, so that the value of the committed bit can be made concealing. Meanwhile, since  $\varepsilon < 1$ , at the end of the commit phase there will be some bits of the string become known to Bob, while Alice does not know the exact position of all these bits. Thus she cannot alter the string freely at a later time, making the protocol binding. The complete QBC protocol is described below.

The *commit* protocol:

- (1) Bob chooses a binary linear  $(n, k, d)$ -code  $C$  [27] and announces it to Alice, where  $n$ ,  $k$ ,  $d$  are agreed on

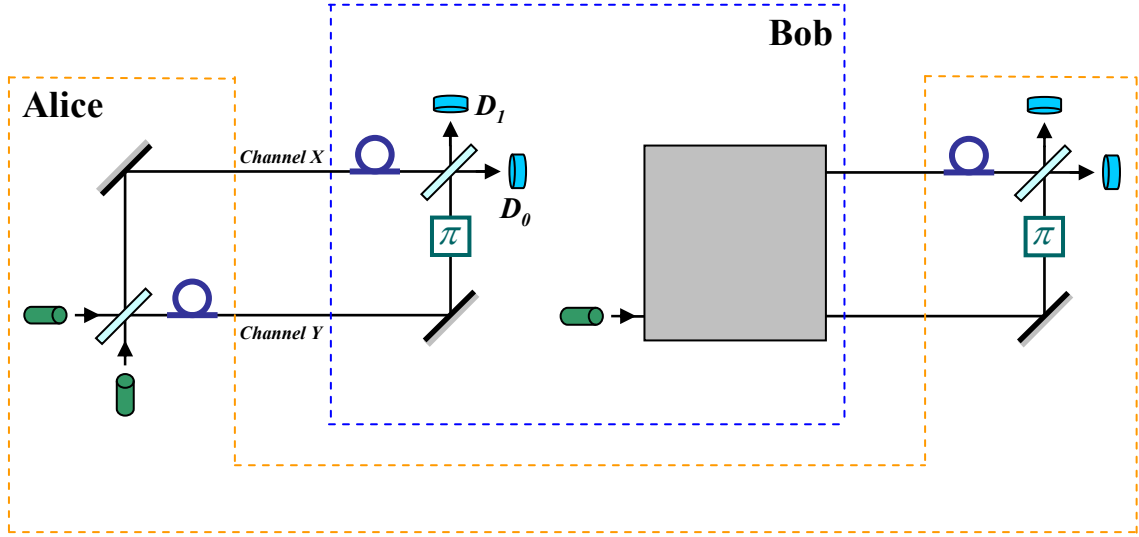


FIG. 2: Diagram for the apparatus of the QBC protocol when Bob chooses the intercept mode. He measures Alice's photon using the same device as that of Alice, while sending another photon to Alice according to a certain strategy (corresponding to the device illustrated as the black box in the diagram) so that Alice's probability of finding his interception can be minimized.

by both Alice and Bob.

(2) Alice chooses a nonzero random  $n$ -bit string  $r = (r_1 r_2 \dots r_n) \in \{0, 1\}^n$  and announces it to Bob. This makes any  $n$ -bit codeword  $c = (c_1 c_2 \dots c_n)$  in  $C$  sorted into either of the two subsets  $C_{(0)} \equiv \{c \in C | c \odot r = 0\}$  and  $C_{(1)} \equiv \{c \in C | c \odot r = 1\}$ . Here  $c \odot r \equiv \bigoplus_{i=1}^n c_i \wedge r_i$ .

(3) Now Alice decides the value of the bit  $b$  that she wants to commit. Then she chooses a codeword  $c$  from  $C_{(b)}$  randomly.

(4) Alice encodes each bit of this specific  $c$  as  $c_i \rightarrow |\Psi_{c_i}\rangle$  where  $|\Psi_{c_i}\rangle$  is defined by equation (1), and sends Bob the two wave packets of the same state separately in channels  $X$  and  $Y$ , with the storage ring  $SR_1$  on channel  $Y$  which introduces a delay time  $\tau$  known to Bob.

(5) For each of Alice's states, Bob chooses the intercept mode with probability  $\alpha$  and the bypass mode with probability  $1 - \alpha$ .

If Bob chooses to apply the bypass mode, he simply keeps channels  $X$  and  $Y$  intact so that the state sent from Alice will be returned to her detectors as-is.

Else if Bob chooses to apply the intercept mode, he uses the same measurement device as that of Alice's, to measure the state so he can decode the corresponding  $c_i$  with certainty. Meanwhile, he prepares another state and sends it back to channels  $X$  and  $Y$  at the right time, so that the time it reaches Alice's detectors will look the same when Bob applies the bypass mode. There could be many different strategies how Bob sends this state (thus we left this part of Bob's device as a black box in FIG. 2). For example, he can use the same device that Alice uses for sending her state. Or he can simply send all wave packets of his state simultaneously in one of the channels alone, e.g., in channel  $X$  beforehand or in channel  $Y$

after his detectors already received Alice's state. But due to the existence of the storage rings in both Alice's sending and measuring devices, if Bob waits until Alice's state enters his site completely, and he measures it then resends the same state to Alice, his resent state will reach Alice's detectors later than it is expected. Therefore, the unconditional security of the KI QKD scheme guarantees that in this mode, once Bob gains non-trivial information on  $c_i$ , his resent state will only have a probability  $1 - \varepsilon < 1$  to make the right detector of Alice click at the right time.

(6) Alice uses the same device that Charlie used in the KI QKD scheme, to measure the output of the quantum channels from Bob. She counts how many times her measurement results do not match the states she sent, and denotes it as  $n'$ . From step (5) it can be seen that  $n' \sim \varepsilon \alpha n$ . Thus Alice can estimate the probability of Bob choosing the intercept mode as  $\alpha \sim n' / (\varepsilon n)$ . Alice agrees to continue with the protocol if  $\alpha < 1 - d/n$ , which means that the number of  $c_i$ 's known to Bob is  $\alpha n < n - d$ . Otherwise she concludes that Bob is cheating.

The *unveil* protocol:

(7) Alice announces the values of  $b$  and  $c = (c_1 c_2 \dots c_n)$ .

(8) Bob accepts the commitment if  $c \odot r = b$  and  $c$  is indeed a codeword from  $C$ , and every  $c_i$  agrees with the state  $|\Psi_{c_i}\rangle$  he detected in the intercept mode.

## V. SECURITY

Intuitively, the protocol is secure against Alice's cheating, because the binary linear  $(n, k, d)$ -code  $C$  guarantees that if Alice wants to change the value of the committed

$b$ , she needs to change at least  $d$  bits of the codeword  $c$ . But she does not know with certainty on which bits Bob has applied the bypass mode. Therefore her probability of altering  $\geq d$  bits without being detected will drop exponentially as  $d$  increases. By fixing  $d/n$  and increasing  $n$  in the protocol, this probability can be made arbitrarily close to zero.

More generally, as pinpointed out in Sec. 4 of [27], the validity of Alice's cheating strategy in all the no-go proofs [3]-[26] of unconditionally secure QBC is based on the condition  $\rho_0^B \simeq \rho_1^B$ , where  $\rho_0^B$  ( $\rho_1^B$ ) is the reduced density matrix of the state sent to Bob during the commit phase when Alice commits  $b = 0$  ( $b = 1$ ). On the other hand, equation (1) shows that in our protocol  $|\Psi_0\rangle$  and  $|\Psi_1\rangle$  are orthogonal. Then the state  $|\psi_c\rangle \equiv |\Psi_{c_1}\rangle \otimes |\Psi_{c_2}\rangle \otimes \dots \otimes |\Psi_{c_i}\rangle \otimes \dots \otimes |\Psi_{c_n}\rangle$  corresponding to a specific codeword  $c$  is orthogonal to the state corresponding to any other codeword. Thus it is clear that our protocol satisfies  $\rho_0^B \perp \rho_1^B$  instead of  $\rho_0^B \simeq \rho_1^B$ , just like the previous protocol in [27], so that they both evade the MLC no-go theorem for the same reason.

The security against Bob is obvious. Step (6) guarantees that during the commit phase, Bob knows  $\alpha n < n - d$  bits of the string  $c$  only. As the  $(n, k, d)$ -code  $C$  ensures that the number of codewords having  $\alpha n$  bits in common grows exponentially as  $k$  increases, knowing  $\alpha n$  bits of  $c$  is insufficient to determine whether  $c$  belongs to  $C_{(0)}$  or  $C_{(1)}$ . Thus Bob does not know  $b$ , and his knowledge on  $b$  can be made arbitrarily small by fixing  $k/n$  and increasing  $n$ . Note that though Alice knows that there are  $n - \alpha n$  bits of  $c$  remaining unknown to Bob before the unveil phase, she does not know the exact position of these bits so she cannot utilize them for cheating.

Though the current QBC protocol and the one in [27] have similarities in many ways, the underlying origins of their security against Bob are somewhat different. While both protocols are immune to Bob's cheating because they are based on unconditionally secure QKD schemes, as pointed out in [30], the GV QKD scheme can actually be viewed as utilizing three orthogonal states – two photon states and one vacuum state. Its security is provided by the random sending times of the photons. On the contrary, the KI QKD scheme does not require the vacuum state. The security is guaranteed by the fact that

the eavesdropper cannot fake the states with certainty owe to the use of the asymmetric beam splitters. Similarly, the security of the QBC protocol in [27] against Bob is based on Alice's random sending times before the last step of the commit phase, while in our current QBC proposal, it is because Bob cannot fake the states with certainty when he runs the intercept mode. Therefore our current protocol is more than merely a simplification on the presentation.

## VI. FEASIBILITY

In the above we focused only on the theoretical possibility of evading the MLC no-go theorem. But we can see from FIG. 2 that our protocol is also very feasible, as the required experimental technology is already available today [31]. Nevertheless, under practical settings, some more security checks should be added against technical attacks. Especially, the physical systems implementing the qubits may actually have other degrees of freedom, which leave rooms for Alice's cheating. For example, she may send photons with certain polarization or frequency, so that she can distinguish them from the photons Bob sends in the intercept mode. In this case, Bob and Alice should discuss at the beginning of the protocol, to limit these degrees of freedom to a single mode. In step (5) when Bob chooses the intercept mode, he should also measure occasionally these degrees of freedom of some of Alice's photons, instead of performing the measurement in the original step (5). Then if Alice wants to send distinguishable photons with a high probability so that they are sufficient for her cheating, she will inevitably be detected.

Also, when Bob applies the bypass mode, he should add phase shifters to both channels  $X$  and  $Y$  to introduce the same phase shift in both channels so that an honest Alice will not be affected, while the amount of this phase shift is randomly chosen and kept secret from Alice, so that the counterfactual attack described in the appendix of [28] can be defeated.

The work was supported in part by the NSF of China under grant No. 10975198, the NSF of Guangdong province, and the Foundation of Zhongshan University Advanced Research Center.

- 
- [1] A. C. C. Yao, in *Proc. 26th Symposium on the Theory of Computing* (ACM, New York, 1995), p.67. Security of quantum protocols against coherent measurements
  - [2] J. Kilian, in *Proc. 1988 ACM Annual Symposium on Theory of Computing* (ACM, New York, 1988), p.20. Founding cryptography on oblivious transfer
  - [3] D. Mayers, *quant-ph/9603015v3*. The trouble with quantum bit commitment
  - [4] D. Mayers, *Phys. Rev. Lett.* **78**, 3414 (1997). Unconditionally secure quantum bit commitment is impossible
  - [5] H. -K. Lo and H. F. Chau, *Phys. Rev. Lett.* **78**, 3410 (1997). Is quantum bit commitment really possible?
  - [6] C. Crépeau, in *Proc. Pragocrypt '96: 1st International Conference on the Theory and Applications of Cryptology* (Czech Technical University Publishing House, Prague, 1996). What is going on with quantum bit commitment?
  - [7] H. F. Chau and H. -K. Lo, *Fortsch. Phys.* **46**, 507 (1998). *quant-ph/9709053v2*. Making an empty promise with a quantum computer
  - [8] H. -K. Lo and H. F. Chau, *Physica D* **120**, 177 (1998). Why quantum bit commitment and ideal quantum coin tossing are impossible

- [9] J. Bub, *Found. Phys.* **31**, 735 (2001). The quantum bit commitment theorem
- [10] G. Brassard, C. Crépeau, D. Mayers, and L. Salvail, *quant-ph/9712023v1*. A brief review on the impossibility of quantum bit commitment
- [11] G. Brassard, C. Crépeau, D. Mayers, and L. Salvail, *quant-ph/9806031v1*. Defeating classical bit commitments with a quantum computer
- [12] R. W. Spekkens and T. Rudolph, *Phys. Rev. A* **65**, 012310 (2001). Degrees of concealment and bindingness in quantum bit commitment protocols
- [13] R. W. Spekkens, and T. Rudolph, *quant-ph/0107042v2*. *Quant. Inf. Comput.* **2**, 66 (2002). Optimization of coherent attacks in generalizations of the BB84 quantum bit commitment protocol
- [14] A. Chailloux and I. Kerenidis, *arXiv:1102.1678v1*. Optimal bounds for quantum bit commitment
- [15] G. M. D'Ariano, *quant-ph/0209149v1*. The quantum bit commitment: a finite open system approach for a complete classification of protocols
- [16] G. M. D'Ariano, *quant-ph/0209150v1*. In *Proc. QCM&C* (Rinton press, Boston, 2002). Shortened version of *quant-ph/0209149*. The quantum bit commitment: a complete classification of protocols
- [17] G. M. D'Ariano, D. Kretschmann, D. Schlingemann, and R. F. Werner, *Phys. Rev. A* **76**, 032328 (2007). *quant-ph/0605224v2*. Reexamination of quantum bit commitment: The possible and the impossible.
- [18] G. Chiribella, G. M. D'Ariano, P. Perinotti, D. M. Schlingemann, and R. F. Werner, *arXiv:0905.3801v1*. A short impossibility proof of quantum bit commitment
- [19] D. Mayers, *quant-ph/0212159v2*. Superselection rules in quantum cryptography
- [20] A. Kitaev, D. Mayers, and J. Preskill, *Phys. Rev. A* **69**, 052326 (2004). Superselection rules and quantum protocols
- [21] H. Halvorson, *J. Math. Phys.* **45**, 4920 (2004). *quant-ph/0310001v2*. Remote preparation of arbitrary ensembles and quantum bit commitment
- [22] C. -Y. Cheung, *quant-ph/0508180v2*. In *Proc. ER-ATO Conference on Quantum Information Science 2005* (Tokyo, 2005). Secret parameters in quantum bit commitment
- [23] C. -Y. Cheung, *quant-ph/0601206v1*. Insecurity of quantum bit commitment with secret parameters
- [24] L. Magnin, F. Magniez, A. Leverrier, and N. J. Cerf, *Phys. Rev. A* **81**, 010302(R) (2010). *arXiv:0905.3419v2*. Strong no-go theorem for Gaussian quantum bit commitment
- [25] G. Chiribella, G. M. D'Ariano, and P. Perinotti, *Phys. Rev. A* **81**, 062348 (2010). *arXiv:0908.1583v5*. Probabilistic theories with purification
- [26] Q. Li, C. -Q. Li, D. -Y. Long, W. H. Chan, and C. -H. Wu, *arXiv:1101.5684v1*. *Quantum Inf. Process.* **11**, 519 (2012). On the impossibility of non-static quantum bit commitment between two parties
- [27] G. P. He, *J. Phys. A: Math. Theor.* **44**, 445305 (2011). Quantum key distribution based on orthogonal states allows secure quantum bit commitment
- [28] G. P. He, *arXiv:1101.4587v3*. Quantum key distribution based on orthogonal states allows secure quantum bit commitment
- [29] L. Goldenberg and L. Vaidman, *Phys. Rev. Lett.* **75**, 1239 (1995). Quantum cryptography based on orthogonal states
- [30] M. Koashi and N. Imoto, *Phys. Rev. Lett.* **79**, 2383 (1997). Quantum cryptography based on split transmission of one-bit information in two steps
- [31] A. Avella, G. Brida, I. P. Degiovanni, M. Genovese, M. Gramegna, and P. Traina, *Phys. Rev. A* **82**, 062309 (2010). Experimental quantum-cryptography scheme based on orthogonal states